Before the
DEPARTMENT OF ENERGY
OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY
WASHINGTON, DC

Smart Grid RFI: Addressing Policy	**)**
and Logistical Challenges	**)**
to Smart Grid Implementation	**)**

COMMENTS OF
THE CENTER FOR DEMOCRACY & TECHNOLOGY
AND THE ELECTRONIC FRONTIER FOUNDATION:
IMPLEMENTING THE FIPS IN THE SMART GRID

I. Introduction

The Center for Democracy & Technology ("CDT")[1] and the Electronic Frontier Foundation ("EFF")[2] are pleased to file these comments in response to the September 17, 2010 Request for Information ("RFI") on "policy and logistical challenges that confront smart grid implementation, as well as recommendations on how to best overcome those challenges."[3]

The RFI focuses in part on the effects on consumers of the implementation of the smart grid. The RFI in particular asks "what role do factors like the trust [and] consumer control … play in shaping consumer participation in [the smart grid]." Clearly, one of the major concerns for consumers in a smart grid setting will be the privacy and security of their data. Addressing this very real concern now, before the widespread implementation of smart grid technology, will not only prevent misuse of consumers' information but also give consumers confidence that their data is secure, thereby encouraging adoption of the new technologies. In particular, the RFI seeks comments regarding "what policies are needed to facilitate the data sharing that will allow … grid automation to achieve [its] potential."[4]

---

[1] CDT is a non-profit, public interest organization with broad experience and expertise in matters of consumer privacy and emerging technologies. CDT has offices in Washington, DC and San Francisco, California.

[2] EFF is a non-profit member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology.

[3] Addressing Policy and Logistical Challenges to Smart Grid Implementation, 75 Fed. Reg. 57006 (2010).

[4] *Id.* at 57010.

Just recently, in connection with a smart grid proceeding in California, CDT and EFF developed concrete and specific policy recommendations for smart grid privacy. Our proposal, attached to this filing as an Appendix, consists of a set of clear but flexible rules that can be incorporated in federal or state regulations, rate orders or other administrative rulings, as well as in grants or contracts.

The California Public Utilities Commission is conducting an in-depth proceeding to spur development of the smart grid in California. Of course, the privacy issue has arisen. Based on extensive filings by CDT and EFF, various parties in the PUC proceeding have agreed,[5] and the Commission has ruled, that the best available framework for developing privacy and security rules for household energy usage data is set of concepts known as the "Fair Information Practice" principles ("FIPs").[6] Similarly, in various federal proceedings on the smart grid, there has been general recognition that privacy rules for the smart grid should be based on the FIPs.

Up until now, however, while everyone has talked about the FIPs, no one has really spelled out what they would mean in reality. That is the challenge that CDT and EFF took on in the California PUC proceeding. In the Appendix to this comment, we offer the results of our work: a clear, concise set of policies and procedures that implement or "operationalize" the full set of FIPs for the smart grid, which we submitted to the California PUC on October 15. We respectfully encourage the Department of Energy to consider these policies and procedures.

In the attached rules, we have put forth a reasonable, balanced and effective approach to privacy that will work across a variety of business models. In drafting these rules, we had in mind at least three different relationships or data flows that might develop for home energy usage information:

- A third party under contract with a utility receives energy usage information from the

---

[5] *E.g.*, Prehearing Conference Statement of Pacific Gas and Electric Company (U 39 E) on Privacy and Security Policies at 2; Prehearing Conference Statement of San Diego Gas & Electric Company's (U 902-E) and Southern California Gas Company (U 904 G) at 8-9; Prehearing Conference Statement of Southern California Edison Company (U 338-E) at 6; Comments of Tendril, Appendix A, p.2 (March 9, 2010) http://docs.cpuc.ca.gov/efile/CM/114794.pdf ("[I]t is recognized that the detailed information required for and generated by the many smart grid technologies and applications will allow far more raw and granular data regarding individual and aggregate energy usage across populations. Such a change raises obvious and non-trivial privacy concerns that we discuss in more detail in these comments.").

[6] *See, e.g.*, Joint Comments of CDT and EFF (March 9, 2010) available at http://www.cdt.org/files/pdfs/20100309_smartgrid_cpuc_comments.pdf. All of the CDT-EFF smart grid filings are compiled here: http://cdt.org/grandchild/smart-grid.

utility and uses that information to provide services on behalf of the utility. Since the third party is a contractor of the utility, customer consent should not be required for the utility to disclose information to this third party initially, but the customer should receive notice of the practice, and the third party should be bound by all the rules that would apply to the utility, including limits on secondary use and onward disclosure. For services not essential to the provision of electrical service, such as demand response, energy management, and energy efficiency services, the customer should be able to opt-out of sharing with the third party.

- A third party receives energy usage information from the utility, but does not provide services on behalf of the utility. Disclosure to this third party should require express, prior, written authorization, in a form we describe in our proposed rules, and the third party should be subject to data security requirements, limits on secondary uses and onward disclosure without consent, and other limits.
- A third party receives energy usage information directly from the customer. The rules we outline should also be extended to these third parties.

II. The Department of Energy Should Adopt, and Encourage States to Adopt, Specific Policies and Procedures Conforming to the Fair Information Practice (FIPs) Principles Detailed Here

In preparation for the transition to the smart grid, the Department of Energy and various state public utility commissions have recognized the need to develop privacy rules suited to the more granular data that will be generated as part of the smart grid and that will flow to a wider range of users beyond the traditional utilities.[7] Moreover, it is increasingly widely recognized that the traditional model for consumer privacy, based on "notice and choice," is inadequate.[8] In the context of the Smart Grid, a notice-and-choice-based approach could leave customers uninformed about the many ways in which their household energy data is being collected and

[7] *E.g.* California Public Utility Commission Assigned Commissioner's and Administrative Law Judge's Joint Ruling of July 30, 2010 at 5; Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy, 75 Fed. Reg. 26203 (2010).

[8] Steve Lohr, Redrawing the Route to Online Privacy, N.Y. Times, Feb. 27, 2010, at BU4 ("'There are essentially no defenders anymore of the pure notice-and-choice model,' said Daniel J. Weitzner, a senior policy official at the National Telecommunications and Information Administration of the Commerce Department. 'It's no longer adequate.'").

used. Notice-and-choice also fails to address other important issues, such as accuracy and security. In contrast, the full FIPs framework includes eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Data Security, and Accountability and Auditing.[9] Each principle protects a unique and vital aspect of customer privacy. Although the full FIPs framework incorporates elements of notice-and-choice, it also fills serious gaps found in pure notice-and-choice regimes.

A. In a Range of Contexts, It is Increasingly Being Recognized that Pure Notice-and-Choice Regimes Are Insufficient for Protecting Customer Privacy

Notice-and-choice regimes are premised on the idea that privacy is best protected by informing customers of how their information is being collected and used and by giving them choices based upon that information. Notice and choice are important and essential values, but they are insufficient by themselves to protect privacy in real-world situations. As recently noted by a Commerce Department official, "[t]here are essentially no defenders anymore of the pure notice-and-choice model."[10] Customers rarely read privacy notices issued by companies, largely due to the length and complexity of those policies.[11] Even if customers do read privacy policies, most are "essentially unusable as decision-making aids,"[12] either because they are difficult to understand[13] or because the service itself is conditioned upon consent to their contents. This failure reflects the privacy policies themselves, not customer apathy. When customers learn

[9] *See, e.g.,* Joint Comments of CDT and EFF (March 9, 2010), supra note 7 at 15-22 (describing the full set of FIPs in greater detail).

[10] Lohr, *supra* note 8, at BU4.

[11] *See* Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP (2008), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf at 2.

[12] Carlos Jensen & Colin Pitts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, 6 Proceedings of the SIGCHI conference on human factors in computing systems 471, 477 (2004), *available at* http://delivery.acm.org/10.1145/990000/985752/p471-jensen.pdf .

[13] *See* An Interview with David Vladeck of the F.T.C., N.Y. TIMES, Aug. 5, 2009, *available at* http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc ("Disclosures are now written by lawyers, they're 17 pages long. I don't think they're written principally to communicate information; they're written defensively…. And I don't believe that most consumers either read them, or, if they read them, really understand it.").

how their information is collected and used, they are concerned and want more control.[14] Indeed, the Federal Trade Commission (FTC) has begun to file actions of deceptive business practices against firms employing insufficient policies based on notice-and-choice.[15] As the FTC's Director of Consumer Protection recently noted, "I'm not sure that consent really reflects a volitional, knowing act."[16] In sum, experts agree that notice and choice alone are insufficient to safeguard customer privacy.

B. In Contrast to the Current Patchwork of Privacy Laws, the FIPs Provide a Clear, Comprehensive Framework to Protect Customer Privacy

One of the major problems facing privacy protection on both the state and federal level is the patchwork coverage provided by existing law. Our research for the California PUC found that even in California, a state that is considered to have strong state privacy laws, existing regulations provide only partial safeguards for customer privacy, with gaps that leave customers vulnerable. Rules addressing the privacy of utility records are contained in the California Public Utilities Code § 394, the Business and Professions Code,[17] and the Information Practices act of 1977.[18] The latest addition to the Public Utilities Code, section 8380 (previously Senate Bill 1476),[19] specifies some additional rules for smart grid data.

Overall, California has a welter of regulations concerning privacy, some of which apply to smart grid entities. However, this patchwork creates neither comprehensive protection for

---

[14] *See e.g.,* Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll* (June 9, 2010), *available at* http://precursorblog.com/content/americans-want-online-privacy-new-zogby-poll.

[15] *See In the Matter of Sears Holdings Management Corporation*, FTC File No. 082 3099, *available at*: http://www.ftc.gov/opa/2009/09/sears.shtm (arguing that even full disclosure of its practices was deceptive when buried in a "lengthy user license agreement, available to consumers at the end of a multi-step registration process").

[16] *See* An Interview with David Vladeck of the F.T.C., *supra* note 16.

[17] BUS. & PROF. CODE § 22575 (requiring privacy policies to be posted by operators of Web sites or online services who collect "personally identifiable information").

[18] *See* CAL. CIVIL CODE § 1798.1(a) ("The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies."); CAL. CIV. CODE § 1798.1(b) ("The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.").

[19] *See* Senate Bill No. 1476, Chapter 497, Statutes of 2010, *available at* http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1451-1500/sb_1476_bill_20100929_chaptered.pdf.

customers nor a clear framework for smart grid entities to follow in protecting customers' information. This example almost certainly holds true across the states and the federal government. A comprehensive framework such as we present in the Appendix can help mitigate this confusion of regulation.

C. Present Privacy Practices of Utilities and Third Parties Operating in California Are Insufficient to Protect Customer Privacy in Smart Grid Data

The insufficiency of the current patchwork quilt is well-illustrated by the experience in California, where our limited review of current practices for energy data shows why current law and the notice-and-choice approach will not fully protect customers in the smart grid environment. To begin with, companies today often do not even have readily accessible notices of their data practices. [20] Moreover, where relevant policies are available, they are often underspecified—lacking, for example, definitions for critical terms, such as the types of energy usage data protected.[21] Few current policies provide users with granular controls, and most give users only the option to cancel service, rather than the opportunity to make meaningful choices about their data use.[22] Although policies often list purposes for which data will be used, those purposes are often so broadly stated (e.g., "to provide you with a better experience")[23] as to allow virtually limitless uses of the data. No energy service policy that we were able to collect

[20] We sought to collect privacy policies concerning energy usage data and/or web usage data from PG&E, SCE, SDG&E and Google PowerMeter. We focused on California as part of a public utility commission proceeding there. We were unable to access energy data polices for two of the three IOUs: SDG&E has a privacy policy for only web usage, *available at* http://www.sdge.com/privacy/; SCE has a privacy policy for only web usage, *available at* http://www.sce.com/PrivacyPolicy/. We requested, but were unable to obtain prior to this filing, SDG&E's and SCE's policies related to *energy data or services*. PG&E, however, does provide an easily accessible policy covering energy data or services on its website, *available at* http://www.pge.com/about/company/privacy/customer.

[21] *E.g.*, PG&E's privacy policy interchangeably uses the terms "customer information," "personal information," "personally identifiable information," and "personal customer information" without defining those terms, *available at* http://www.pge.com/about/company/privacy/customer.

[22] *E.g.*, neither Google PowerMeter's nor PG&E's policy allows users to opt-out of any parts of the policy except through cancellation, *available at* http://www.google.com/powermeter/privacy and http://www.pge.com/about/company/privacy/customer.

[23] Google Privacy Policy (effective date Oct. 3, 2010), *available at* http://www.google.com/privacypolicy_2010.html (stating that it may use data to "to provide you with a better experience and to improve the quality of our services"); see also PG&E's Privacy Policy, *available at* http://www.pge.com/about/company/privacy/customer (stating that it may use data "to manage, provide, and improve our services and business operations").

explains whether the information collected from customers is limited to the minimum amount needed to fulfill any stated purpose, or mentions remedial procedures for managing data breaches or other security violations. Thus, under the present circumstances, even diligent customers may not understand the notice provided; if they do, existing policies are unlikely to provide them with full information or meaningful choices.

III. CDT and EFF Have Developed a Clear, Reasonable and Effective Implementation of the FIPs for the Smart Grid

To be effective, the FIPs principles must take concrete form. Only then will all of the parties—customers, utilities, and third parties—tangibly understand their rights and responsibilities. As such we recommend to the Department of Energy and the various stakeholders the specific requirements attached hereto as Appendix A. In developing the proposal, we attempted to protect the privacy of customers and provide clear standards without placing undue burden on smart grid service providers.

Our proposal improves on the traditional notice and consent model in important ways. Under "Transparency" and "Purpose Specification," it ensures that customers will receive *specific* information about who collects, receives, stores, or uses their data, and for what purposes each entity uses the data. Under the principle of "Individual Participation," it affirms customers' right to access their own data and to challenge its accuracy. Our proposal draws a distinction between primary purposes and secondary purposes, and ties use and disclosure limits to those concepts, making it clear that utilities do not need consent to collect, retain, or use data for purposes directly related to the provision of electrical or gas service to the customer, but that prior express authorization is needed for disclosure to third parties not providing service on behalf of the utility and for other secondary uses.[24] In a vast improvement over many current privacy policies, we make it clear that customer consent is specific to each third party and to each purpose. In another improvement, under "Data Minimization," the proposal ties the amount of data collected and disclosed to the specified purposes, in order to minimize the amount of

[24] SB 1476 contemplates that energy usage data may be disclosed with customer consent for secondary commercial purposes. Our proposed rules specify how such consent should be obtained. However, SB 1476 does not define secondary commercial uses, nor does it suggest that the concept is limitless. The Commission may address whether some secondary commercial purposes should be precluded entirely.

unnecessary customer data collected or disclosed by utilities and third parties.[25] Finally, the proposal addresses disclosure pursuant to legal process[26] and requires reasonable security protections and basic accountability.

IV. Conclusion

The Center for Democracy & Technology and the Electronic Frontier Foundation commend the Department of Energy on its careful consideration of the consumer issues presented by the emerging smart grid, including those regarding privacy. We urge the Department to consider the privacy proposals set out in the Appendix. These proposals implement the full set of FIPs that many have recognized as critical to safeguarding customer privacy.

Respectfully submitted this November 1, 2010 at Washington, DC.

James X. Dempsey
Center for Democracy & Technology
55 New Montgomery St. #513
San Francisco, CA 94105
415-814-1712

Lee Tien
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415-436-9333 x 102

[25] While our recommendation focuses on a rule-oriented framework for data minimization, the flow of energy usage data from the home can also be minimized by the very design or architecture of consumer energy management systems. We thus urge the Commission to recognize that "it is possible to protect consumer privacy at a macro level by choosing a system design that minimizes frequent access to granular data from outside the consumer site" and to seek information from parties to this proceeding about such possibilities. *See* NISTIR 7628, GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 36-37 (Aug. 2010) (using the example of intelligent gateways that can both optimize energy consumption and prevent pattern recognition against known load profiles).

[26] The proposal, in accordance with existing law, directs covered entities, in the absence of consent, not to disclose energy usage data except pursuant to a warrant or court order. While our proposal does not separately address standards for government access in criminal investigations versus standards for access in civil litigation, we believe that in cases where very detailed data is being sought in the course of a criminal investigation, a warrant will be required. The Supreme Court, in *Kyllo v. United States*, 533 U.S. 27 (2001) held that a warrant is required to use an infrared device to collect what is in essence energy usage data (the heat signature of a home), where the information being collected was detailed enough to permit inferences about what was going on inside the home. Justice Scalia, in writing for the majority, stated: "In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes. Thus, in *Karo*, *supra*, the only thing detected was a can of ether in the home; and in *Arizona* v. *Hicks*, 480 U.S. 321 (1987), the only thing detected by a physical search that went beyond what officers lawfully present could observe in "plain view" was the registration number of a phonograph turntable. These were intimate details because they were details of the home, just as was the detail of how warm—or even how relatively warm—Kyllo was heating his residence." *Kyllo* at 37-38.

APPENDIX A – Privacy Policies and Procedures

1. Definitions

(a) **Covered Entity.** A "covered entity" is (1) any electrical service provider, electric corporation, gas corporation or community choice aggregator, or (2) any third party that collects, stores, uses, or discloses covered information [relating to 100 or more households or residences].[27]

(b) **Covered Information.** "Covered information" is any energy usage information concerning an individual, family, household, or residence, except that covered information does not include information from which identifying information has been removed such that it cannot reasonably be identified or re-identified with an individual, family, household, or residence.

(c) **Primary Purposes.** The "primary purposes" for the collection, storage, use or disclosure of covered information are to—
  (1) provide or bill for electrical power,
  (2) fulfill other operational needs of the electrical system or grid, and
  (3) implement demand response, energy management, or energy efficiency programs operated by, or on behalf of and under contract with, an electric or gas corporation.

(d) **Secondary Purpose.** "Secondary purpose" means any purpose that is not a primary purpose.

2. Transparency (Notice)

(a) **Generally.** Covered entities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the collection, storage, use, and disclosure of covered information.

(b) **When Provided.** Covered entities shall provide notice in their first paper correspondence with the customer, if any, and shall provide conspicuous posting of the notice on the home page of their website.

(c) **Form.** The notice shall be labeled "Privacy Policy: Notice of Collection, Storage, Use and Disclosure of Energy Usage Information" and shall—
  (1) be written in easily understandable language,
  (2) be no longer than is necessary to convey the requisite information.

(d) **Content.** The notice shall state clearly—
  (1) the identity of the covered entity,
  (2) the effective date of the notice,
  (3) the covered entity's process for altering the notice, including how the customer will be informed of any alterations, and where prior versions will be made available to customers, and
  (4) the title and contact information, including email address, postal address, and telephone number, of an official at the covered entity who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or distribution of covered information.

---

[27] Comment: Some further thought needs to be given to the interplay between this threshold and the rules for legal process; we are concerned about unregulated governmental access to energy usage information from landlords of smaller apartment buildings.

3. PURPOSE SPECIFICATION The notice required under section 2 shall provide—

(a) an explicit description of—
  (1) each category of covered information collected, used, stored or disclosed by the covered entity, and, for each category of covered information, the specific purposes for which it will be collected, stored, used, or disclosed, and
  (2) each category of covered information that is disclosed to third parties, and, for each category, (i) the purposes for which it is disclosed, (ii) the identities of the third parties to which it is disclosed, and (iii) the value of the disclosure to the customer;

(b) the periods of time that covered information is retained by the covered entity;

(c) a description of the choices available to customers and the means by which they may exercise those choices, including the means by which they may—
  (1) view, inquire about, or dispute their covered information, and
  (2) limit the collection, use, storage or disclosure of covered information; and

(d) the consequences to the customer, if any, of refusing consent to the covered entity, in whole or in part, regarding the collection, storage, use, or distribution of covered information.

4. INDIVIDUAL PARTICIPATION (ACCESS AND CONTROL)

(a) **Access.** Covered entities shall provide to customers convenient and secure access to their covered information—
  (1) in an easily readable format that is at a level of detail sufficient for the customer to utilize reasonably available energy management or energy efficiency products, but in no event at a level less detailed than that at which the covered entity discloses the data to third parties for demand response, energy management or energy efficiency purposes.
  (2) The Commission shall, by subsequent rule, prescribe what is a reasonable time for responding to customer requests for access.

(b) **Control.** Covered entities shall provide customers with convenient mechanisms for—
  (1) granting and revoking authorization for secondary uses of their covered information,
  (2) disputing the accuracy or completeness of covered information that the covered entity is storing or distributing for any primary or secondary purpose, and
  (3) requesting corrections or amendments to covered information that the covered entity is collecting, storing, using, or distributing for any primary or secondary purpose.

(c) **Disclosure Pursuant to Legal Process.**

(1) Except as otherwise provided in this rule or expressly authorized by law, a covered entity shall not disclose covered information except pursuant to a warrant or other court order naming with specificity the customers whose information is sought. Unless otherwise directed by a court, covered entities shall treat requests for real-time access to covered information as wiretaps, requiring approval under the federal or state wiretap law.

(2) Unless otherwise prohibited by court order, a covered entity, upon receipt of a

demand for disclosure of covered information, shall, prior to complying, notify the customer in writing and allow the customer 7 days to appear and contest the claim of the person or entity seeking disclosure.
(3) Nothing in this rule prevents a person or entity seeking energy usage information from demanding such information from the customer under any applicable legal procedure or authority.
(4) Nothing in this section prohibits a covered entity from disclosing covered information with the consent of the customer, where the consent is express, written and specific to the purpose and to the person or entity seeking the information.
(5) Nothing in this rule prevents a covered entity from disclosing, in response to a subpoena, the name, address and other contact information regarding a customer.
(6) On an annual basis, covered entities shall report to the Commission the number of times that customer data has been sought without consent, and for each such instance, whether it was a civil or criminal case, whether the covered entity complied with the request as initially presented or as modified in form or scope, and how many customers' records were disclosed. The Commission should make such reports publicly available.

5. DATA MINIMIZATION

(a) **Generally.** Covered entities shall collect, store, use, and disclose only as much covered information as is necessary to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.
(b) **Data Retention.** Covered entities shall maintain covered information only for as long as necessary to accomplish a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.
(c) **Data Disclosure.** Covered entities shall not disclose to any third party more covered information than is necessary to carry out on behalf of the covered entity a specific primary purpose identified in the notice required under section 2 or for a specific secondary purpose authorized by the customer.

6. USE AND DISCLOSURE LIMITATION

(a) **Generally.** Covered information shall be used solely for the purposes specified by the covered entity in accordance with section 3.
(b) **Primary Purposes.** A gas or electric corporation may use covered information for primary purposes without customer consent.
(c) **Disclosures to Third Parties.** A gas or electric corporation may disclose covered information to a third party when the third party is performing a primary purpose on behalf of a gas or electrical corporation, provided that the gas or electric corporation shall, by contract, require the third party to collect, store, use, and disclose covered information under policies and practices no less protective than those under which the gas or electric corporation itself operates and, if the information is being disclosed for [demand response], energy management or energy efficiency purposes, the gas or electric corporation permits customers to opt-out of such disclosure.

(d) **Secondary Purposes**. No covered entity shall use or disclose covered information for any secondary purpose without obtaining the customer's prior, express, written authorization for each such purpose, provided that authorization is not required when information is—
   (1) provided to a law enforcement agency in response to lawful process;
   (2) required by the Commission pursuant to its jurisdiction and control over electric and gas corporations.

(e) **Customer Authorization.**
   (1) **Authorization.** Separate authorization must be obtained for each secondary purpose.
   (2) **Revocation.** Customers have the right to revoke, at any time, any previously granted authorization.
   (3) **Expiration.** Customer consent shall be deemed to expire after two years, after which time customers will need to reauthorize any secondary purposes.

(f) **Parity.** Covered entities shall permit customers to cancel authorization for any secondary use of their covered information by the same mechanism initially used to grant authorization.

7. DATA QUALITY AND INTEGRITY

Covered entities shall ensure that covered information they collect, store, use, and disclose is accurate and complete.

8. DATA SECURITY

(a) **Generally.** Covered entities shall implement appropriate administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(b) **Breach.** Covered entities shall disclose any breach in accordance with section 1798.82 of the Information Practices Act. In addition, covered entities shall notify the Commission of breaches of covered information.

9. ACCOUNTABILITY AND AUDITING

(a) **Generally**. Covered entities shall be accountable for complying with the principles herein, and must file with the Commission—
   (1) the privacy notices that they provide to customers,
   (2) their internal privacy and security policies,
   (3) the identities of agents, contractors and other third parties to which they disclose covered information, the purposes for which that information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose, and
   (4) copies of any secondary-use authorization forms by which the covered party secures customer authorization for secondary uses of covered data.

(b) **Redress.** Covered entities shall provide customers with mechanisms for appropriate access to covered information, for correction of inaccurate covered information, and for redress in the event of a violation of these rules.

(c) **Training**. Covered entities shall provide appropriate training to all employees and contractors who use, store or process covered information.

(d) **Audits**. Covered entities shall conduct an independent audit of security and privacy practices at least once per year to monitor compliance with its privacy and security commitments, and shall report the findings to the Commission.

(e) **Disclosures**. On an annual basis, covered entities shall disclose to the Commission—

(1) the number and identities of authorized third parties accessing customer energy usage information,

(2) the number of security breaches experienced by the electrical corporation or gas corporation, and

(3) the number and percentage of customers affected by breaches of covered information.